

GENUS FIELDS OF ABELIAN EXTENSIONS OF CONGRUENCE RATIONAL FUNCTION FIELDS

MYRIAM MALDONADO-RAMÍREZ, MARTHA RZEDOWSKI-CALDERÓN,
AND GABRIEL VILLA-SALVADOR

ABSTRACT. We give a construction of genus fields for congruence function fields. First we consider the cyclotomic function field case following the ideas of Leopoldt and then the general case. As applications we give explicitly the genus fields of Kummer, Artin-Schreier and cyclic p -extensions. Kummer extensions were obtained previously by G. Peng and Artin-Schreier extensions were obtained by S. Hu and Y. Li.

1. INTRODUCTION

The concept of genus field goes back to Gauss [4] in the context of binary quadratic forms. For any finite extension K/\mathbb{Q} , the genus field is defined as the maximal unramified extension K_g of K such that K_g is the composite of K and an abelian extension k^* of \mathbb{Q} : $K_g = Kk^*$. This definition is due to Frölich [3]. If K_H denotes the Hilbert class field of K , $K \subseteq K_g \subseteq K_H$. Originally the definition of genus field was given for a quadratic extension of \mathbb{Q} . Gauss in fact proved that if t is the number of different positive finite rational primes dividing the discriminant δ_K of a quadratic number field K , then the 2-rank of the class group of K is 2^{t-2} if $\delta_K > 0$ and there exists a prime $p \equiv 3 \pmod{4}$ dividing δ_K and 2^{t-1} otherwise.

H. Leopoldt [8] determined the genus field K_g of an abelian extension K of \mathbb{Q} using Dirichlet characters, generalizing the work of H. Hasse [5] who introduced genus theory for quadratic number fields.

M. Ishida determined the genus field K_g of any finite extension of \mathbb{Q} [7]. X. Zhang [14] gave a simple expression of K_g for any abelian extension K of \mathbb{Q} using Hilbert ramification theory.

For function fields, the notion of Hilbert class field has no proper analogue since the maximal abelian extension of any congruence function field K/\mathbb{F}_q contains $K_m := K\mathbb{F}_{q^m}$ for all positive integers m and therefore the maximal unramified abelian extension of K is of infinite degree over K .

M. Rosen [10] gave a definition of an analogue of the Hilbert class field of K and a fixed finite nonempty set S_∞ of prime divisors of K . Using this definition, a proper concept of genus field can be given along the lines of the classical case. R. Clement [2] considered a cyclic extension of $k := \mathbb{F}_q(T)$ of degree a prime number l dividing $q-1$ and found the genus field using class field theory. Later, S. Bae and J. Koo [1] generalized the results of Clement following the methods of Frölich [3].

Date: June 21, 2012.

1991 Mathematics Subject Classification. Primary 11R60; Secondary 11R29, 11R58.

Key words and phrases. Genus fields, congruence function fields, global fields, Dirichlet characters, cyclotomic function fields, Kummer extensions, Artin-Schreier extensions, Witt vectors.

G. Peng [9] explicitly described the genus theory for Kummer function fields. Recently S. Hu and Y. Li [6] explicitly described the ambiguous ideal class and the genus of an Artin–Schreier extension of a congruence rational function field.

In this paper we develop an analogue of Leopoldt’s genus theory for congruence function fields. We give a description of the genus field K_g of a finite abelian extension of a congruence rational function field by means of the group of Dirichlet characters for cyclotomic function fields. Here we consider the Hilbert class field K_H of a function field K using the construction of Rosen for $S_\infty = \{\mathfrak{p}_\infty\}$, where \mathfrak{p}_∞ is the pole divisor of T in the rational function field $k = \mathbb{F}_q(T)$.

More precisely, let K be a finite abelian extension of k . Then if K is contained in a cyclotomic extension, we find that K_g is also contained in a cyclotomic extension and we find the group of characters associated to K_g . If K is not contained in a cyclotomic extension and \mathfrak{p}_∞ is tamely ramified, we consider a suitable extension of constants of K and then proceed as before to find K_g . Finally, if \mathfrak{p}_∞ is wildly ramified we consider the cyclotomic extension where \mathfrak{p}_∞ is totally and wildly ramified and proceed similarly to the previous cases.

We apply our results to Kummer and to Artin–Schreier extensions of k and we give new proofs of the results of Peng and of Hu and Li. At the end, we show that our construction also works to find explicitly the genus field of an arbitrary finite cyclic p -extension of k given by a Witt vector.

2. CLASSICAL CASE

Let K be a number field, that is, a finite extension of \mathbb{Q} . Let K_H be the Hilbert class field of K , that is, K_H is the maximal abelian unramified extension of K . Then the genus field K_g of K is the maximal extension of K contained in K_H that is the composite of K and an abelian extension k^* of \mathbb{Q} . Equivalently, $K_g = Kk^* \subseteq K_H$ with k^* the maximal abelian extension of \mathbb{Q} contained in K_H .

First we recall genus theory in the abelian case for number fields [8]. In this case K_g is the maximal extension of K contained in K_H such that K_g/\mathbb{Q} is abelian. So, in this section we consider K/\mathbb{Q} an abelian extension. By the Kronecker–Weber Theorem there exists $n \in \mathbb{N}$ such that $K \subseteq \mathbb{Q}(\zeta_n)$, where ζ_n denotes a primitive n -th root of unity. Let X be the group of Dirichlet characters associated to K . That is, X is a subgroup of the dual of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong U_n := (\mathbb{Z}/n\mathbb{Z})^*$; then $X \subseteq \hat{U}_n$ and K is the subfield of $\mathbb{Q}(\zeta_n)$ fixed by $\cap_{\chi \in X} \ker \chi$.

Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the factorization of n as a product of prime powers. For any character χ let $\chi_{p_i} = \chi \circ \varphi_i$

$$\begin{array}{ccc} U_n & \xrightarrow{\chi} & \mathbb{C}^* \\ \varphi_i \uparrow & \nearrow \chi_{p_i} & \\ U_{p_i^{\alpha_i}} & & \end{array}$$

where $\varphi_i = \Phi^{-1} \circ g_{p_i}$, with

$$\begin{array}{ll} \Phi: U_n \rightarrow \prod_{j=1}^r U_{p_j^{\alpha_j}} & \text{and} \quad g_{p_i}: U_{p_i^{\alpha_i}} \rightarrow \prod_{j=1}^r U_{p_j^{\alpha_j}} \\ a \bmod n \mapsto (a \bmod p_j^{\alpha_j})_j & a \bmod p_i^{\alpha_i} \mapsto (1, \dots, a \bmod p_i^{\alpha_i}, \dots, 1). \end{array}$$

The character χ_{p_i} has conductor $p_i^{\beta_i}$ for some $\beta_i \in \mathbb{N}$, $1 \leq i \leq r$. For any rational prime $p \notin \{p_1, \dots, p_r\}$, $\chi_p = 1$. Let p be a rational prime and define $X_p := \{\chi_p \mid \chi \in X\}$. Then we have $|X_p| = e_p$ is the ramification index of p in K . Thus,

Theorem 2.1 (Leopoldt [8]). *Let K be an abelian extension of \mathbb{Q} and let X be the group of Dirichlet characters associated to K . Let J be the maximal abelian extension of \mathbb{Q} containing K such that J/K is unramified at every finite rational prime. Let Y be the group of Dirichlet characters associated to J . Then $Y = \prod_{p \in \mathcal{P}} X_p$, where the product runs through the set of rational primes \mathcal{P} .*

Proof. Since J/K is not ramified in any finite prime, we have $e_p(J/K) = 1$, then the ramification indices coincide, thus $|X_p| = |Y_p|$ for all primes p . Since $X_p \subseteq Y_p$, we have $X_p = Y_p$. Let $Z := \prod_{p \in \mathcal{P}} X_p$. Then $Z_p = X_p$. Let F be the field associated to Z . As $X \subseteq \prod_{p \in \mathcal{P}} X_p = Z$, we have $K \subseteq F$ and analogously $J \subseteq F$. On the other hand, since $|X_p| = |Z_p|$, the extension F/K is unramified, thus $F \subseteq J$. Therefore $F = J$ and it follows that $Y = Z = \prod_{p \in \mathcal{P}} X_p$. \square

Remark 2.2. If the infinite primes are unramified in J/K we have $K_g = J$. Otherwise, K is real and J is imaginary. Then $K_g = J^+$ where $J^+ := J \cap \mathbb{R}$ and the group of Dirichlet characters associated to J^+ is $Y^+ := \{\chi \in Y \mid \chi(-1) = 1\}$. Finally $[J : J^+] = [Y : Y^+] = 2$.

Example 2.3 (Gauss Genus Theorem). Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension of \mathbb{Q} , where $d \in \mathbb{Z}$ is square free. Let m be the number of different prime factors of δ_K , the discriminant of K . If p_1, \dots, p_m are these factors, we choose $p_1 = 2$ if $2 \mid \delta_K$.

Let χ be the quadratic character associated to K . Then $\chi_{p_i} \neq 1$, $1 \leq i \leq m$ and $\chi_q = 1$ for all $q \in \mathcal{P} \setminus \{p_1, \dots, p_m\}$. For $p_i \neq 2$, χ_{p_i} is unique and $\chi_{p_i}(-1) = (-1)^{(p_i-1)/2}$. In this case the field associated to χ_{p_i} is $\mathbb{Q}(\sqrt{(-1)^{(p_i-1)/2} p_i})$. If $p_1 = 2$, then there are three quadratic characters $\chi_{p_1} = \chi_2$; two of them have conductor 8, one is real and one imaginary, and the other one has conductor 4. If χ_2 is real, $\chi(-1) = 1$ and the field associated is $\mathbb{Q}(\sqrt{2})$. If χ_2 is imaginary of conductor 8, $\chi(-1) = -1$ and the field associated is $\mathbb{Q}(\sqrt{-2})$. Finally, if χ_2 is of conductor 4, $\chi(-1) = -1$ and the field associated to χ_2 is $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. It follows that the maximal abelian extension of \mathbb{Q} unramified at every finite prime is $J = \mathbb{Q}(\sqrt{\varepsilon}, \sqrt{(-1)^{(p_i-1)/2} p_i} \mid 2 \leq i \leq m)$ where $\varepsilon = (-1)^{(p_1-1)/2} p_1$ if $p_1 \neq 2$ and $\varepsilon = 2, -2$ or -1 if $p_1 = 2$.

Thus we obtain $[J : \mathbb{Q}] = 2^m$ and $[J : K] = 2^{m-1}$. We have $K_g = J$ except when K is real and J is imaginary and this last case occurs when $\delta_K > 0$ ($d > 0$) and there exists $p_i \equiv 3 \pmod{4}$. In this case, $[J^+ : K] = 2^{m-2}$. For the quadratic extension $K = \mathbb{Q}(\sqrt{-14})$ over \mathbb{Q} , we have $K_g = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ and for $K = \mathbb{Q}(\sqrt{79})$ we obtain $J = \mathbb{Q}(\sqrt{-79}, i)$ and $K_g = J^+ = J \cap \mathbb{R} = \mathbb{Q}(\sqrt{79}) = K$.

Now if \mathcal{C}_K is the class group of K , $\mathcal{C}_K \cong \text{Gal}(K_H/K)$ and E is the fixed field of \mathcal{C}_K^2 , then $\text{Gal}(E/K) \cong \mathcal{C}_K/\mathcal{C}_K^2$. Since K_g is the maximal abelian extension of \mathbb{Q} contained in K_H , K_g is the fixed subfield of K_H under the derived group G' of $G := \text{Gal}(K_H/\mathbb{Q})$. It can be verified that $G' = \mathcal{C}_K^2$ so that $K_g = E$ and it follows that the 2-rank of \mathcal{C}_K is 2^{m-1} unless $d > 0$ and there exists a prime $p \equiv 3 \pmod{4}$ dividing d and in this case the 2-rank of \mathcal{C}_K is 2^{m-2} .

Example 2.4. If p is an odd prime, K is a cyclic extension of \mathbb{Q} of degree p and m is the number of ramified primes in K , it follows that K_g is an elementary abelian p -extension of \mathbb{Q} of degree p^m and $[K_g : K] = p^{m-1}$. In particular $p^{m-1} \mid |\mathcal{C}_K|$.

Now let K be any abelian extension of \mathbb{Q} with Dirichlet character group X . Consider for each $p \in \mathcal{P}$, X_p . Let J be the field associated to $\prod_{p \in \mathcal{P}} X_p$. Let $p^{m_p} := \gcd\{f_{\chi_p} \mid \chi \in X\}$ where f_{χ_p} denotes the conductor of χ_p . Then the field K_p associated to X_p is contained in $\mathbb{Q}(\zeta_{p^{m_p}})$ but not in $\mathbb{Q}(\zeta_{p^{m_p-1}})$. If p is odd, K_p is the unique subfield of $\mathbb{Q}(\zeta_{p^{m_p}})$ of degree $|X_p|$ over \mathbb{Q} and K_p/\mathbb{Q} is a cyclic extension. If $p = 2$, K_2 is one of the following fields. If $|X_2| = \varphi(2^{m_2}) = 2^{m_2-1}$, $K_2 = \mathbb{Q}(\zeta_{2^{m_2}})$. If $|X_2| = \frac{\varphi(2^{m_2})}{2} = 2^{m_2-2}$, $K_2 = \mathbb{Q}(\zeta_{2^{m_2}})^+ = \mathbb{Q}(\zeta_{2^{m_2}} + \zeta_{2^{m_2}}^{-1}) = \mathbb{Q}(\zeta_{2^{m_2}}) \cap \mathbb{R}$ if $\chi(-1) = 1$ for all $\chi \in X$ and $K_2 = \mathbb{Q}(\zeta_{2^{m_2}} - \zeta_{2^{m_2}}^{-1})$ if there exists $\chi \in X$ with $\chi(-1) = -1$.

Therefore, if K and J are both real or both imaginary, $K_g = J = \prod_{p \in \mathcal{P}} K_p$. If K is real and J is imaginary, $K_g = J^+ = J \cap \mathbb{R}$.

3. CYCLOTOMIC FUNCTION FIELDS

First we give some notations and some results in the theory of cyclotomic function fields [13]. Let $k = \mathbb{F}_q(T)$ be a congruence rational function field, \mathbb{F}_q denoting the finite field of q elements. Let $R_T = \mathbb{F}_q[T]$ be the ring of polynomials, that is, R_T is the ring of integers of k . R_T^+ denotes the set of monic irreducible polynomials in R_T . For $N \in R_T \setminus \{0\}$, Λ_N denotes the N -torsion of the Carlitz module and $k(\Lambda_N)$ denotes the N -th cyclotomic function field. The R_T -module Λ_N is cyclic and λ_N , or λ if there is no possible confusion, denotes a generator of Λ_N as R_T -module. For any function field K/\mathbb{F}_q , $K_m := K\mathbb{F}_{q^m}$ denotes the constant field extension. For any $m \in \mathbb{N}$, C_m denotes a cyclic group of order m .

We have $k(\Lambda_N) = k(\lambda_N)$ and $G_N := \text{Gal}(k(\Lambda_N)/k) \cong (R_T/(N))^*$ with the identification $\sigma_A \lambda_N = \lambda_N^A$ for $A \in R_T$. For any finite extension K/k we will use the symbol $S_\infty(K)$ to denote either one prime or all primes in K above \mathfrak{p}_∞ , the pole divisor of T in k . We understand by a *Dirichlet character* any group homomorphism $\chi: (R_T/(N))^* \rightarrow \mathbb{C}^*$ and we define the conductor f_χ of χ as the monic polynomial of minimum degree such that χ can be defined modulo f_χ , $\chi: (R_T/(f_\chi))^* \rightarrow \mathbb{C}^*$.

Given any group of characters $X \subseteq \widehat{G_N} (= \text{hom}(G_N, \mathbb{C}^*))$, the field associated to X is the subfield of $k(\Lambda_N)$ fixed under $\cap_{\chi \in X} \ker \chi$. Conversely, for any field $K \subseteq k(\Lambda_N)$, the group of Dirichlet characters associated to K is $\widehat{\text{Gal}(K/k)}$.

For any character χ we consider the canonical decomposition $\chi = \prod_{P \in R_T^+} \chi_P$, where χ_P has conductor a power of P . We have $f_\chi = \prod_{P \in R_T^+} f_{\chi_P}$.

If X is a group of Dirichlet characters, we write $X_P := \{\chi_P \mid \chi \in X\}$ for $P \in R_T^+$. If K is any extension of k , $k \subseteq K \subseteq k(\Lambda_N)$ and $P \in R_T^+$, then the ramification index of P in K is $e_P = |X_P|$.

In $k(\Lambda_N)/k$, \mathfrak{p}_∞ has ramification index $q-1$ and decomposes into $\frac{|G_N|}{q-1}$ different prime divisors of $k(\Lambda_N)$ of degree 1. Furthermore, with the identification $G_N \cong (R_T/(N))^*$, the inertia (= decomposition) group \mathfrak{I} of \mathfrak{p}_∞ is $\mathbb{F}_q^* \subseteq (R_T/(N))^*$, that is, $\mathfrak{I} = \{\sigma_a \mid a \in \mathbb{F}_q^*\}$. The primes that ramify in $k(\Lambda_N)/k$ are \mathfrak{p}_∞ and the polynomials $P \in R_T^+$ such that $P \mid N$.

We set L_n to be the largest subfield of $k(\Lambda_{1/T^n})$ where \mathfrak{p}_∞ is fully and purely wildly ramified, $n \in \mathbb{N}$. For any field F , ${}_n F$ denotes the composite FL_n .

We recall Rosen's definition for a relative Hilbert class field of a congruence function field K .

Definition 3.1 ([10]). Let K be a function field with field of constants \mathbb{F}_q . Let S be any nonempty finite set of prime divisors of K . The *Hilbert class function field of K relative to S* , $K_{H,S}$, is the maximal unramified abelian extension of K where every element of S decomposes fully.

From now on, for any finite extension K of k we will consider S as the set of prime divisors dividing \mathfrak{p}_∞ , the pole divisor of T in k and we write K_H instead of $K_{H,S}$.

Definition 3.2. Let K be a finite geometric extension of k . The *genus field* K_g of K is the maximal extension of K contained in K_H that is the composite of K and an abelian extension of k . Equivalently, $K_g = Kk^*$ where k^* is the maximal abelian extension of k contained in K_H .

When K/k is an abelian extension, K_g is the maximal abelian extension of k contained in K_H . Our main goal in this section is to find K_g when K is a subfield of a cyclotomic function field. In what follows K will always denote a finite geometric abelian extension of k . First we note that we have the analogue to Leopoldt's result.

Proposition 3.3. *If $K \subseteq k(\Lambda_N)$ and the group of characters associated to K is X , then the maximal abelian extension J of K unramified at every finite prime $P \in R_T^+$, contained in a cyclotomic extension, is the field associated to $Y = \prod_{P \in R_T^+} X_P = \prod_{P|N} X_P$.*

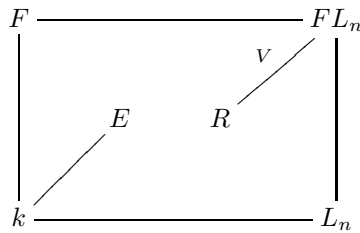
Proof. Analogous to the proof of Theorem 2.1. \square

In this case \mathfrak{p}_∞ has no inertia in J/K but it might be ramified.

Proposition 3.4. *If E/k is an abelian extension such that \mathfrak{p}_∞ is tamely ramified, then there exist $N \in R_T$ and $m \in \mathbb{N}$ such that $E \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$.*

Proof. By the Kronecker–Weber Theorem [13, Theorem 12.8.5], we have $E \subseteq k(\Lambda_N)\mathbb{F}_{q^m}L_n = {}_nk(\Lambda_N)_m$ for some $N \in R_T$ and $n, m \in \mathbb{N}$.

Let $F := k(\Lambda_N)\mathbb{F}_{q^m} = k(\Lambda_N)_m$ and let V be the first ramification group of \mathfrak{p}_∞ in FL_n/k . Then $R := (FL_n)^V$ is the maximal extension of k where \mathfrak{p}_∞ is tamely



ramified and in consequence $S_\infty(R)$ is wildly ramified in FL_n/R .

Since \mathfrak{p}_∞ is tamely ramified in E/k , it follows that $E \subseteq R$. Now, \mathfrak{p}_∞ is tamely ramified in F/k and $S_\infty(F)$ is fully and wildly ramified in FL_n/F and FL_n/F is of degree $|V|$. Hence $R = F$ and $E \subseteq F$. \square

Proposition 3.5. *With the hypothesis of Proposition 3.3, if $e_{\mathfrak{p}_\infty}(K|k) = q - 1$, then $K_g = J$.*

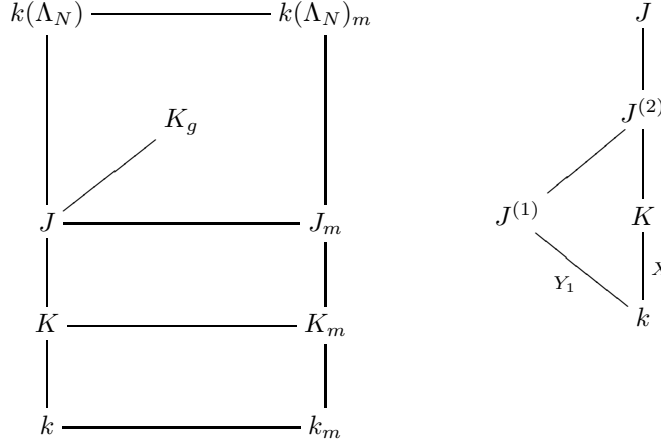
Proof. Since $e_{\mathfrak{p}_\infty}(J|K) = \frac{e_{\mathfrak{p}_\infty}(J|k)}{e_{\mathfrak{p}_\infty}(K|k)} = \frac{q-1}{q-1} = 1$, \mathfrak{p}_∞ decomposes fully in J/K and therefore $J \subseteq K_g$.

Now the field of constants of K_g is \mathbb{F}_q (see [10] or simply if \mathbb{F}_{q^m} is the field of constants of K_g , $k \subseteq k_m \subseteq K_g$ and \mathfrak{p}_∞ is fully inert in k_m ; since \mathfrak{p}_∞ and $S_\infty(K)$ have no inertia in either K/k or J/K , $m = 1$.)

Since \mathfrak{p}_∞ decomposes fully in K_g/K and \mathfrak{p}_∞ is tamely ramified in K/k , by Proposition 3.4 we have $K_g \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$ for some $N \in R_T$ and $m \in \mathbb{N}$.

In all the extensions k_m/k , K_m/K , J_m/J , $k(\Lambda_N)_m/k(\Lambda_N)$ the infinite primes are fully inert since all have degree 1 (see [13, Theorem 6.2.1]). In the extensions K_m/k_m and K/k the ramification index of the infinite primes is $q - 1$, that is, the maximal possible. It follows that in J_m/K_m , J/K , $k(\Lambda_N)/J$ and $k(\Lambda_N)_m/J_m$, $S_\infty(K_m)$, $S_\infty(K)$, $S_\infty(J)$ and $S_\infty(J_m)$ are fully decomposed. Finally, in $k(\Lambda_N)_m/J$ (and therefore in $k(\Lambda_N)_m/K_g$), $S_\infty(J)$ is unramified.

Let $\mathcal{G} := \text{Gal}(k(\Lambda_N)_m/J)$. For $S_\infty(J)$ we have that in this extension the ramification index e , the inertia degree f and the decomposition number h are $e = 1$, $f = m$ and $h = \frac{|\mathcal{G}|}{m}$. Therefore the decomposition group \mathfrak{D} of \mathfrak{p}_∞ is of order m and it is cyclic. We must have $\mathfrak{D} = \text{Gal}(k(\Lambda_N)_m/k(\Lambda_N))$ because $S_\infty(k(\Lambda_N))$ is fully inert of degree m in $k(\Lambda_N)_m/k(\Lambda_N)$. Since $S_\infty(J)$ has inertia degree 1 in K_g/J , it follows that $K_g \subseteq k(\Lambda_N)$. Thus $K_g = J$. \square



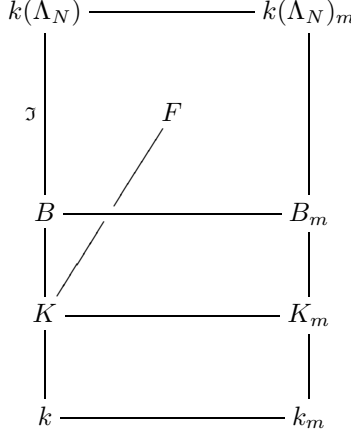
Now we consider the general case $k \subseteq K \subseteq k(\Lambda_N)$. We use the notations of Proposition 3.3. In this case \mathfrak{p}_∞ might be ramified in J/K . Let $Y_1 := \{\chi \in Y \mid \chi(a) = 1 \text{ for all } a \in \mathbb{F}_q^* \subseteq (R_T/(N))^* \cong G_N\}$ and let $J^{(1)}$ be the field associated to Y_1 . Then $J^{(1)} \subseteq J$ since $Y_1 \subseteq Y$, though not necessarily $J^{(1)} \subseteq K$ or $K \subseteq J^{(1)}$. Let $J^{(2)} := KJ^{(1)}$.

Then $J^{(2)}$ is the field associated to the character group XY_1 . Since \mathfrak{p}_∞ decomposes fully in $J^{(1)}/k$, $S_\infty(K)$ decomposes fully in $J^{(2)}$. Furthermore $S_\infty(J^{(1)})$ is fully ramified in $J/J^{(1)}$. Hence $S_\infty(J^{(2)})$ is fully ramified in $J/J^{(2)}$.

We obtain that $J^{(2)}/K$ is an unramified abelian extension with $J^{(2)} \subseteq k(\Lambda_N)$ and $S_\infty(K)$ decomposes fully in $J^{(2)}/K$. It follows that $J^{(2)} = J^{\mathfrak{D}}$ where \mathfrak{D} is the decomposition group of $S_\infty(J)$.

Now consider any unramified abelian extension F/K such that $S_\infty(K)$ decomposes fully in F . By Proposition 3.4, $F \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$ for some $N \in R_T$ and $m \in \mathbb{N}$. In case $F \subseteq k(\Lambda_N)$, let Z be the group of Dirichlet characters associated to F . Since F/K is unramified, it follows that $X \subseteq Z \subseteq Y$ by Proposition 3.3 and thus

$F \subseteq J$. Since $J^{(2)} = J^{\mathfrak{D}}$, we obtain that $F \subseteq J^{(2)}$.



For the general case $k \subseteq F \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$, let \mathfrak{I} be the inertia group of $S_\infty(K)$ in $k(\Lambda_N)/K$ and let $B := k(\Lambda_N)^{\mathfrak{I}}$. Then $S_\infty(B)$ is fully inert in B_m because it has degree 1 and $S_\infty(B)$ is fully ramified in $k(\Lambda_N)/B$. Since $S_\infty(K)$ decomposes fully in B , B is the decomposition field of $S_\infty(K)$ in $k(\Lambda_N)_m/K$ so $F \subseteq B \subseteq k(\Lambda_N)$.

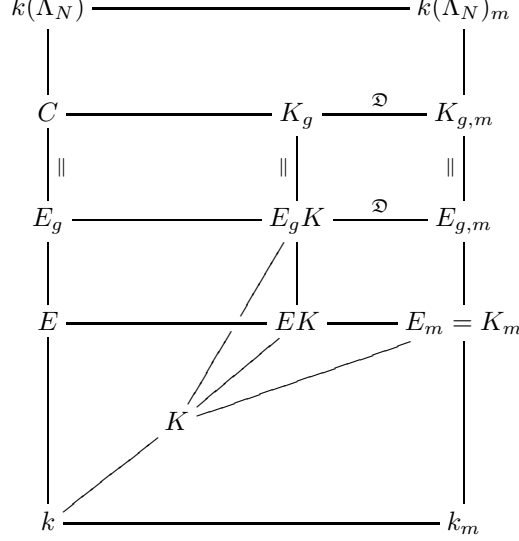
From the first part, we obtain that $F \subseteq J^{(2)}$. We have proved the following

Theorem 3.6. *Assume $K \subseteq k(\Lambda_N)$ for some polynomial N . Let X be the group of Dirichlet characters associated to K , $Y = \prod_{P|N} X_P$, $Y_1 = \{\chi \in Y \mid \chi(a) = 1 \text{ for all } a \in \mathbb{F}_q^*\}$ and $J^{(1)}$ the field associated to Y_1 . Then the genus field K_g of K satisfies $K_g \subseteq k(\Lambda_N)$ and $K_g = KJ^{(1)}$. \square*

4. GENERAL CONGRUENCE FUNCTION FIELDS

First we consider any finite geometric abelian extension K/\mathbb{F}_q of k such that \mathfrak{p}_∞ is tamely ramified. Then we have $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m} = k(\Lambda_N)_m$ for some $N \in R_T$ and $m \in \mathbb{N}$. Since $k(\Lambda_N)/k$ is a geometric extension and k_m/k is an extension of constants, we have $k(\Lambda_N) \cap k_m = k$. Define $E := K_m \cap k(\Lambda_N) \subseteq K_m$. Thus $E_m \subseteq K_m$. On the other hand $[K_m : k] = [K_m : k_m][k_m : k] = [E : k][k_m : k] = [E_m : k_m][k_m : k] = [E_m : k]$. Therefore $E_m = K_m$. We also have $[E : k] = [K : k]$ since $m[K : k] = [K_m : k] = [E_m : k] = m[E : k]$. In other words, E plays a role similar to that of K but it is contained in a cyclotomic extension.

Since $E = K_m \cap k(\Lambda_N)$, it follows that $E \cap K = E_g \cap K = k(\Lambda_N) \cap K$. Because K_m/K and E_g/E are unramified, we obtain that $E_g K/K$ is unramified. Also, since $S_\infty(E)$ decomposes fully in E_g , $S_\infty(EK)$ decomposes fully in $E_g K$. Now, $S_\infty(E \cap K)$ has inertia degree one in $E/(E \cap K)$ so $S_\infty(K)$ has inertia degree one in EK/K . Therefore $E_g K \subseteq K_g$. Finally, if $C := K_g \cap k(\Lambda_N)$, on the one hand $E_g \subseteq C$ and on the other hand C/E is unramified since K_g/EK and EK/E are unramified; also $S_\infty(E)$ decomposes fully in C/E . It follows that $C \subseteq E_g$. Thus, $C = E_g$ and $K_g = E_g K$.



Note that $K_{g,m} = E_{g,m}$. Hence $K_g = E_{g,m}^{\mathfrak{D}}$ where \mathfrak{D} is the decomposition group of $S_{\infty}(K)$ in $E_{g,m}/K$. Observe that $|\mathfrak{D}| = [K_{g,m} : K_g] = \frac{m}{t}$ where t is the degree of $S_{\infty}(K)$.

We have proved

Theorem 4.1. *Let K/\mathbb{F}_q be a geometric finite abelian extension of k where \mathfrak{p}_{∞} is tamely ramified. Let $N \in R_T$ and $m \in \mathbb{N}$ be such that $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$. Let E_g be the genus field of $E := k(\Lambda_N) \cap K\mathbb{F}_{q^m}$ and let $E_{g,m} = E_g\mathbb{F}_{q^m}$. Let \mathfrak{D} be the decomposition group of $S_{\infty}(K)$ in $E_{g,m}$. Then the genus field of K is $K_g = E_{g,m}^{\mathfrak{D}} = E_g K$. \square*

Remark 4.2. Let $\langle \sigma \rangle = \text{Gal}(k(\Lambda_N)_m/k(\Lambda_N)) \cong \text{Gal}(k_m/k)$. Then with the above notations, we have $\mathfrak{D} \cong \langle \sigma^t \rangle$ and

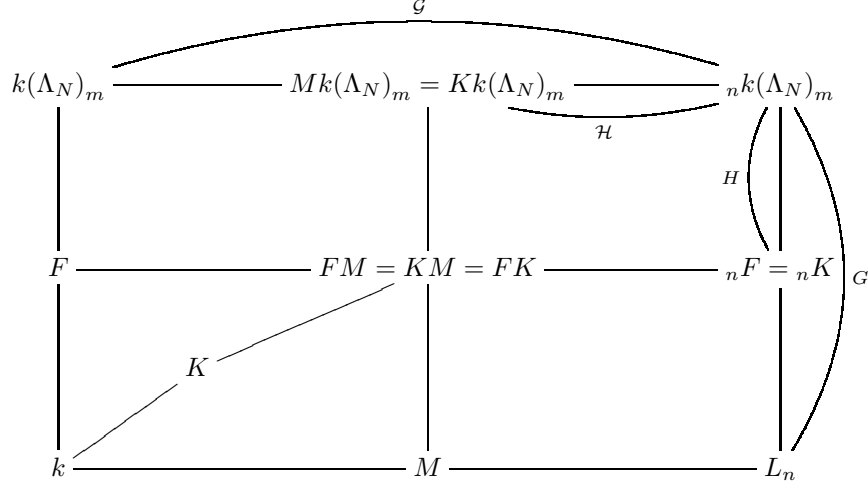
$$[K_g : K] = \frac{[E_{g,m} : K]}{|\mathfrak{D}|} = \frac{[E_{g,m} : K_m][K_m : K]}{m/t} = [E_g : E]t,$$

where $t = \deg(S_{\infty}(K))$.

Finally we consider any geometric finite abelian extension K of k . By the Kronecker–Weber Theorem, we have $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m}L_n = {}_n k(\Lambda_N)_m$ for some $N \in R_T$ and $n, m \in \mathbb{N}$. Let $\mathcal{G} := \text{Gal}({}_n k(\Lambda_N)_m/k(\Lambda_N)_m)$, $\mathcal{H} := \text{Gal}({}_n k(\Lambda_N)_m/Kk(\Lambda_N)_m)$, $M := Kk(\Lambda_N)_m \cap L_n = L_n^{\mathcal{H}_1}$ where $\mathcal{H}_1 := \mathcal{H}|_{L_n}$.

Let $G := \text{Gal}({}_n k(\Lambda_N)_m/L_n)$, $H := \text{Gal}({}_n k(\Lambda_N)_m/{}_n K)$, $F := {}_n K \cap k(\Lambda_N)_m = k(\Lambda_N)_m^{H_1}$ where $H_1 := H|_{k(\Lambda_N)_m}$.

We have $F = {}_n K \cap k(\Lambda_N)_m \subseteq {}_n K$. Hence, on the one hand ${}_n F \subseteq {}_n K$, and on the other hand $[{}_n k(\Lambda_N)_m : {}_n F] = [k(\Lambda_N)_m : F] = |H_1| = |H| = [{}_n k(\Lambda_N)_m : {}_n K]$. It follows that ${}_n F = {}_n K$. Similarly we obtain $Mk(\Lambda_N)_m = Kk(\Lambda_N)_m$.



Set $A \subseteq \mathcal{G} \times G$ such that $K = {}_nk(\Lambda_M)_m^A$. First we will prove that $FM = KM = FK$. We have $F = {}_nk(\Lambda_N)_m^{\mathcal{G} \times H}$ and $M = {}_nk(\Lambda_N)_m^{\mathcal{H} \times G}$. Then if we denote $R = {}_nk(\Lambda_N)_m$, we have

$$\begin{aligned} R^{A \cap (\mathcal{G} \times 1)} &= R^A R^{\mathcal{G} \times 1} = Kk(\Lambda_N)_m = Mk(\Lambda_N)_m \\ &= R^{\mathcal{H} \times G} R^{\mathcal{G} \times 1} = R^{(\mathcal{H} \times G) \cap (\mathcal{G} \times 1)} = R^{\mathcal{H} \times 1}, \end{aligned}$$

so that $A \cap (\mathcal{G} \times 1) = \mathcal{H} \times 1$. Similarly $A \cap (1 \times G) = 1 \times H$. Therefore

$$\begin{aligned} FM &= R^{\mathcal{G} \times H} R^{\mathcal{H} \times G} = R^{(\mathcal{G} \times H) \cap (\mathcal{H} \times G)} = R^{\mathcal{H} \times H}, \\ KM &= R^A R^{\mathcal{H} \times G} = R^{A \cap (\mathcal{H} \times G)}, \\ FK &= R^{\mathcal{G} \times H} R^A = R^{(\mathcal{G} \times H) \cap A}. \end{aligned}$$

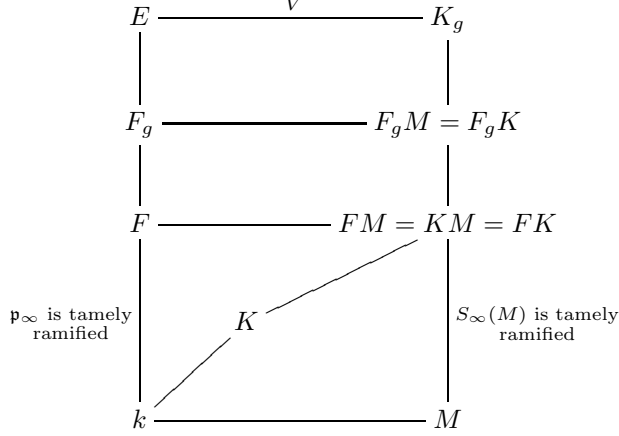
Since it is easily seen that $(\mathcal{G} \times H) \cap A = A \cap (\mathcal{H} \times G) = \mathcal{H} \times H$, it follows that $FM = KM = FK$.

Given that F_g/F is unramified and $S_\infty(F)$ decomposes fully, we obtain that ${}_nKF_g/{}_nK$ is unramified and $S_\infty({}_nF)$ decomposes fully. Now, in ${}_nK/K$ the only possible ramified prime is $S_\infty(K)$ and if this is so, it is wildly ramified. It follows that in ${}_nKF_g/K$ the only possible ramified prime is $S_\infty(K)$ and if this is so, it is wildly ramified. In particular in F_gK/K the only possible ramified prime is $S_\infty(K)$ and if it ramified, it is wildly ramified.

Again, given that the extension F_g/F is unramified and $S_\infty(F)$ decomposes fully, F_gK/FK is unramified and $S_\infty(FK)$ decomposes fully. In the extension $F/(K \cap F)$, $S_\infty(K \cap F)$ is tamely ramified, hence $S_\infty(K)$ is tamely ramified in FK/K . Therefore $S_\infty(K)$ decomposes fully in FK/K . In short, we have $F_gK \subseteq K_g$.

Since $FM = FK$, $F_gM = F_gK \subseteq K_g$. Let V be the first ramification group of \mathfrak{p}_∞ in K_g/k . Set $E := K_g^V$. Then \mathfrak{p}_∞ is tamely ramified in E/k and therefore $E \subseteq k(\Lambda_N)_m$. We obtain that $S_\infty(M)$ is tamely ramified in K_g/M and since K_g/K is unramified, it follows that K_g/FM is unramified. Finally \mathfrak{p}_∞ is tamely ramified in F/k so $S_\infty(M)$ is tamely ramified in FM/M . Since \mathfrak{p}_∞ is fully and wildly

ramified in M/k , $M \cap E = k$.



Now $[K_g : k] = [E : k]|V| = [E : k][M : k] = [EM : k]$. It follows that $K_g = EM$. We also have $F_g \subseteq E$ because $F_g = F_g K \cap E \subseteq E$. The extension $K_g/F_g K$ is unramified so K_g/FK is unramified and the only possible ramified prime in $FK = FM/F$ is $S_\infty(F)$ and if it is so, it is wildly ramified. $S_\infty(F)$ is not ramified in E/F since otherwise it would be tamely ramified, and E/F is unramified at every other prime because K_g/F is ramified at most at $S_\infty(F)$. It follows that $E \subseteq F_g$ and therefore $E = F_g$. Thus $K_g = EM = F_g M = F_g K$.

We have proved

Theorem 4.3. *Let K/k be any finite abelian extension with $K \subseteq {}_n k(\Lambda_N)_m$. Let $F = {}_n K \cap k(\Lambda_N)_m$ and $M = Kk(\Lambda_N)_m \cap L_n$. Then the genus field of K is $K_g = F_g K = F_g M$.* \square

Our main result is the combination of Theorems 4.1 and 4.3.

Theorem 4.4. *Let K/k be a finite abelian extension with $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m}L_n$. Let $F = KL_n \cap k(\Lambda_N)\mathbb{F}_{q^m}$ and $E = k(\Lambda_N) \cap F\mathbb{F}_{q^m} \subseteq k(\Lambda_N)$. Then the genus field of K is $K_g = E_g FK$ where E_g is the genus field of E .* \square

5. APPLICATIONS

In this section we will see how our results can be applied to some general abelian extensions: Kummer, Artin–Schreier and p -cyclic (Witt) extensions.

5.1. Kummer Extensions. Here we will assume that $q \geq 3$. Let $P \in R_T^+$. Then $k(\sqrt[q-1]{(-1)^{\deg P} P}) \subseteq k(\Lambda_N)$ (see [11, Lemma 16.13]). Thus for l a prime number such that $l \mid q-1$, we have $k(\sqrt[l]{(-1)^{\deg P} P}) \subseteq k(\Lambda_P)$. Therefore for any monic polynomial $D \in R_T$, we obtain $k(\sqrt[l]{(-1)^{\deg D} D}) \subseteq k(\Lambda_D)$.

Note that for $\alpha, \beta \in \mathbb{F}_q^*$, we have $k(\sqrt[l]{\alpha D}) = k(\sqrt[l]{\beta D})$ iff $\alpha \equiv \beta \pmod{(\mathbb{F}_q^*)^l}$. In particular $k(\sqrt[l]{\gamma D}) \subseteq k(\Lambda_D)$ iff $\gamma \equiv (-1)^{\deg D} \pmod{(\mathbb{F}_q^*)^l}$. It follows that if $l \mid \deg D$ then $k(\sqrt[l]{D}) \subseteq k(\Lambda_D)$.

In this subsection we use the notations of Section 4. Let $K := k(\sqrt[l]{\gamma D})$ with $D \in R_T$ a monic l -power free polynomial, $\gamma \in \mathbb{F}_q^*$ and $D = P_1^{e_1} \cdots P_r^{e_r}$ where $P_i \in R_T^+$, $1 \leq e_i \leq l-1$, $1 \leq i \leq r$. Furthermore we arrange the product so that

$l \mid \deg P_i$ for $1 \leq i \leq s$ and $l \nmid \deg P_j$ for $s+1 \leq j \leq r$, $0 \leq s \leq r$. In general, we always have $E = k(\sqrt[l]{(-1)^{\deg D} D})$, and $\mathbb{F}_q^* \subseteq (\mathbb{F}_{q^l}^*)^l$.

Proposition 5.1. *The behavior of \mathfrak{p}_∞ in K/k is the following:*

- (a).- *If $l \nmid \deg D$, \mathfrak{p}_∞ is ramified.*
- (b).- *If $l \mid \deg D$ and $\gamma \in (\mathbb{F}_q^*)^l$, \mathfrak{p}_∞ decomposes.*
- (c).- *If $l \mid \deg D$ and $\gamma \notin (\mathbb{F}_q^*)^l$, \mathfrak{p}_∞ is inert.*

Proof. [9, Lemma 3] □

Now by Remark 4.2, we have $[K_g : K] = [E_g : E]t$ where

$$t = \deg S_\infty(K) = \begin{cases} 1 & \text{if } \mathfrak{p}_\infty \text{ is not inert in } K/k, \\ l & \text{if } \mathfrak{p}_\infty \text{ is inert in } K/k. \end{cases}$$

When $K = E$, that is, when $K \subseteq k(\Lambda_D)$, if χ is the character of order l associated to K , $\chi = \chi_{P_1} \cdots \chi_{P_r}$, we consider $Y = \langle \chi_{P_i} \mid 1 \leq i \leq r \rangle$. The field associated to Y is $F = k(\sqrt[l]{(-1)^{\deg P_1} P_1}, \dots, \sqrt[l]{(-1)^{\deg P_r} P_r})$, and $K_g = F$ if $l \nmid \deg D$ or if $l \mid \deg P_i$ for all i (that is, $s = r$). This is because in the first case \mathfrak{p}_∞ is already ramified in K and in the second \mathfrak{p}_∞ is unramified in F/k (Proposition 5.1).

When $l \mid \deg D$ and $l \nmid \deg P_r$, \mathfrak{p}_∞ ramifies in F/k and is unramified in E/k . In this case $[F : E_g] = l$. Let $a_{s+1}, \dots, a_{r-1} \in \mathbb{Z}$ be such that $l \mid \deg(P_i P_r^{a_i})$, that is, $\deg P_i + a_i \deg P_r \equiv 0 \pmod{l}$, $s+1 \leq i \leq r-1$. Let

$$F_1 := k(\sqrt[l]{P_1}, \dots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1} P_r^{a_{s+1}}}, \dots, \sqrt[l]{P_{r-1} P_r^{a_{r-1}}}) \subseteq k(\Lambda_{P_1 P_2 \cdots P_r}).$$

Then $S_\infty(E)$ decomposes in F_1/E , $K \subseteq F_1 \subseteq E_g$ and since $F = F_1(\sqrt[l]{(-1)^{\deg P_r} P_r})$, we have $[F : F_1] = l$. It follows that $E_g = F_1$.

In the general case, from Theorem 4.3 we obtain $K_g = E_g K$. Therefore

Theorem 5.2 (G. Peng [9]). *Let $D = P_1^{e_1} \cdots P_r^{e_r} \in R_T$ be a monic l -power free polynomial, where $P_i \in R_T^+$, $1 \leq e_i \leq l-1$, $1 \leq i \leq r$. Let $0 \leq s \leq r$ be such that $l \mid \deg P_i$ for $1 \leq i \leq s$ and $l \nmid \deg P_j$ for $s+1 \leq j \leq r$. Let $K := k(\sqrt[l]{\gamma D})$ where $\gamma \in \mathbb{F}_q^*$. Then K_g is given by:*

- (a).- $k(\sqrt[l]{\gamma D}, \sqrt[l]{(-1)^{\deg P_1} P_1}, \dots, \sqrt[l]{(-1)^{\deg P_r} P_r})$ if $l \nmid \deg D$ or if $l \mid \deg P_i$ for all $1 \leq i \leq r$,
- (b).- $k(\sqrt[l]{\gamma D}, \sqrt[l]{P_1}, \dots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1} P_r^{a_{s+1}}}, \dots, \sqrt[l]{P_{r-1} P_r^{a_{r-1}}})$, where the exponent a_j satisfies $\deg P_j + a_j \deg P_r \equiv 0 \pmod{l}$, $s+1 \leq j \leq r-1$, if $l \mid \deg D$ and $l \nmid \deg P_r$. □

5.2. Artin-Schreier extensions. Consider $K := k(y)$ where $y^p - y = \alpha \in k$. The equation can be normalized as:

$$(5.1) \quad y^p - y = \alpha = \sum_{i=1}^r \frac{Q_i}{P_i^{e_i}} + f(T),$$

where $P_i \in R_T^+$, $Q_i \in R_T$, $\gcd(P_i, Q_i) = 1$, $e_i > 0$, $p \nmid e_i$, $\deg Q_i < \deg P_i^{e_i}$, $1 \leq i \leq r$, $f(T) \in R_T$, with $p \nmid \deg f$ when $f(T) \notin \mathbb{F}_q$.

We have that the finite primes ramified in K/k are precisely P_1, \dots, P_r . With respect to \mathfrak{p}_∞ we have

Proposition 5.3. *The prime \mathfrak{p}_∞ is*

- (a).- *decomposed if $f(T) = 0$.*

- (b).- *inert if $f(T) \in \mathbb{F}_q$ and $f(T) \notin \wp(\mathbb{F}_q) := \{a^p - a \mid a \in \mathbb{F}_q\}$.*
(c).- *ramified if $f(T) \notin \mathbb{F}_q$ (thus $p \nmid \deg f$).* \square

We study two cases.

Case 1: We assume that \mathfrak{p}_∞ is not ramified, so $f(T) \in \mathbb{F}_q$. We have $\text{Gal}(K_p/k) \cong C_p \times C_p$. The $p+1$ fields of degree p over k contained in K_p are: $k(y + \beta_i)$, $1 \leq i \leq p$ and k_p , where $\{\beta_i\}_{i=1}^p$ is a basis of \mathbb{F}_{q^p} over \mathbb{F}_q . By Proposition 5.3, the unique such extension such that \mathfrak{p}_∞ is not inert is the one $k(w)$ such that $w^p - w = \alpha - f(T)$. Thus $E = k(w)$.

If χ is the character associated to E , then $\chi = \chi_{P_1} \cdots \chi_{P_r}$ and the field associated to χ_{P_i} is $k(y_i)$, where $y_i^p - y_i = \alpha_i := \frac{Q_i}{P_i^{e_i}}$, $1 \leq i \leq r$. Therefore

$$(5.2) \quad E_g = k(y_1, \dots, y_r).$$

Thus $K_g = E_g K = k(y_1, \dots, y_r, \beta)$ with $\beta^p - \beta \notin \wp(\mathbb{F}_q) = \{x^p - x \mid x \in \mathbb{F}_q\}$.

Case 2: Now consider the case \mathfrak{p}_∞ ramified in K . Set $K_1 := k(\beta)$, $\beta^p - \beta = f(T)$, $p \nmid \deg f$. Let $E := k(w)$ where $w^p - w = \alpha - f(T) = \alpha_1 = \sum_{i=1}^r \frac{Q_i}{P_i^{e_i}}$. By Case 1, $E_g = k(y_1, \dots, y_r)$. Therefore $K_g = E_g K = k(y_1, \dots, y_r, \beta)$.

We have proved

Theorem 5.4 (S. Hu and Y. Li [6]). *Let $K = k(y)$ be given by (5.1). Then $K_g = k(y_1, \dots, y_r, \beta)$, where $y_i^p - y_i = \frac{Q_i}{P_i^{e_i}}$, $1 \leq i \leq r$ and $\beta^p - \beta = f(T)$.* \square

5.3. p -cyclic extensions. This case is similar to Artin-Schreier's. Here we consider $K = k(\vec{y})$ where $\vec{y}^p - \vec{y} = \vec{\beta}$, and the operation is the Witt difference. The extension is a finite p -extension of degree less than or equal to p^n where \vec{y} is of length n . Let P_1, \dots, P_r be the finite prime divisors ramified in K/k .

Theorem 5.5. *Let K/k be a cyclic extension of degree p^n where $P_1, \dots, P_r \in R_T^+$ and possibly \mathfrak{p}_∞ , are the ramified prime divisors. Then $K = k(\vec{y})$ where*

$$\vec{y}^p - \vec{y} = \vec{\beta} = \vec{\delta}_1 + \cdots + \vec{\delta}_r + \vec{\mu},$$

with $\beta_1^p - \beta_1 \notin \wp(k)$, $\delta_{ij} = \frac{Q_{ij}}{P_i^{e_{ij}}}$, $e_{ij} \geq 0$, $Q_{ij} \in R_T$ and if $e_{ij} > 0$, then $p \nmid e_{ij}$, $\gcd(Q_{ij}, P_i) = 1$ and $\deg(Q_{ij}) < \deg(P_i^{e_{ij}})$, and $\mu_j = f_j(T) \in R_T$ with $p \nmid \deg f_j$ when $f_j \notin \mathbb{F}_q$.

Proof. We recall some facts on Witt vectors that we will need. In general, for the ring $R := \mathbb{Q}[x_i, y_j, z_l]$ in the variables x_i, y_j, z_l we consider the ring R_n , $n \in \mathbb{N}$ with the underlying set equal to R^n and with the operations $+$, $-$, \cdot componentwise. Let R^n be the ring with underlying set the same R^n and with the following operations (Witt). Let $\varphi: R^n \rightarrow R_n$ be given by $\varphi(a_1, \dots, a_n) = (a^{(1)}, \dots, a^{(n)})$ where

$$a^{(m)} := a_1^{p^{m-1}} + p a_2^{p^{m-2}} + \cdots + p^{m-1} a_m, \quad m = 1, \dots, n.$$

Then φ is a bijective map with inverse $\psi: R_n \rightarrow R^n$ given by $\psi(a^{(1)}, \dots, a^{(n)}) = (a_1, \dots, a_n)$ where

$$a_m = \frac{1}{p^{m-1}} \left(a^{(m)} - a_1^{p^{m-1}} - p a_2^{p^{m-2}} - \cdots - p^{m-2} a_{m-1}^p \right), \quad m = 1, \dots, n.$$

The Witt operations $\dot{+}$, $\dot{-}$ and $\dot{\cdot}$ on R^n are given by

$$a \dot{+} b = \left(a^\varphi \dot{+} b^\varphi \right)^{\varphi^{-1}}.$$

Now we return to our case of congruence function fields. Consider K/k a cyclic extension of degree p^n given by $K := k(\vec{y})$, $\vec{y}^p \dot{-} \vec{y} = \vec{\beta}$ with $\vec{y} \in W_n(K)$ a Witt vector of length n in K and $\vec{\beta} \in W_n(k)$ a Witt vector of length n in k .

Let $\vec{\beta} = (\beta_1, \dots, \beta_n)$ be such that

$$(5.3) \quad \begin{aligned} \beta_j &= \sum_{i=1}^r \frac{Q_{ij}}{P_i^{e_{ij}}} + f_j(T), \text{ where } P_1, \dots, P_r \in R_T^+, \{Q_{ij}\}_{1 \leq j \leq n}^{1 \leq i \leq r} \subseteq R_T, \\ f_j(T) &\in R_T, e_{ij} \in \mathbb{N} \cup \{0\} \text{ for all } 1 \leq i \leq r \text{ and } 1 \leq j \leq n. \end{aligned}$$

Now when we apply φ to $\vec{\beta}$ we obtain $(\beta^{(1)}, \dots, \beta^{(n)})$ and from the definition of $\beta^{(j)}$, we obtain

$$\beta^{(j)} = \sum_{i=1}^r \frac{Q'_{ij}}{P_i^{e'_{ij}}} + f'_j(T) \text{ for all } 1 \leq j \leq n.$$

We write

$$\begin{aligned} \vec{\beta} &= \vec{\gamma}_1 + \dots + \vec{\gamma}_r + \vec{\xi}, \\ (\beta^{(1)}, \dots, \beta^{(n)}) &= (\gamma_1^{(1)}, \dots, \gamma_1^{(n)}) + \dots + (\gamma_r^{(1)}, \dots, \gamma_r^{(n)}) + (\xi^{(1)}, \dots, \xi^{(n)}) \end{aligned}$$

with

$$\gamma_i^{(j)} = \frac{Q'_{ij}}{P_i^{e'_{ij}}}, \quad 1 \leq i \leq r, 1 \leq j \leq n \text{ and } \xi^{(j)} = f'_j(T).$$

When we apply φ^{-1} , we obtain

$$(\beta_1, \dots, \beta_n) = (\beta^{(1)}, \dots, \beta^{(n)})^{\varphi^{-1}} = (\vec{\gamma}_1)^{\varphi^{-1}} \dot{+} \dots \dot{+} (\vec{\gamma}_r)^{\varphi^{-1}} \dot{+} (\vec{\xi})^{\varphi^{-1}}$$

and each vector $(\vec{\gamma}_i)^{\varphi^{-1}}$ is of the form $\left(\frac{Q''_{i1}}{P_i^{e''_{i1}}}, \dots, \frac{Q''_{in}}{P_i^{e''_{in}}}\right)$ and the vector $(\vec{\xi})^{\varphi^{-1}}$ is of the form $(f''_1(T), \dots, f''_n(T))$. In other words

$$\vec{\beta} = \vec{\delta}_1 \dot{+} \dots \dot{+} \vec{\delta}_r \dot{+} \vec{\mu}$$

where the components of each $\vec{\delta}_i$ have poles at most at P_i and $\vec{\mu}$ has components with poles at most at \mathfrak{p}_∞ . Let \mathfrak{p}_i be the divisor corresponding to P_i .

Now each $\vec{\delta}$ and $\vec{\mu}$ can be normalized in such a way that each component $(\vec{\delta}_i)_j := \delta_{ij}$ has divisor

$$\begin{aligned} (\delta_{ij})_k &= \frac{\mathfrak{a}_{ij}}{\mathfrak{p}_i^{\lambda_i}} \text{ with } \lambda_i \geq 0; \text{ if } \lambda_i = 0, \text{ then } v_{\mathfrak{p}_i}(\mathfrak{a}_{ij}) \geq 0; \\ \text{if } \lambda_i > 0, \text{ then } \gcd(p, \lambda_i) &= 1 \text{ and } v_{\mathfrak{p}_{ij}}(\mathfrak{a}_{ij}) = 0, \end{aligned}$$

and similarly for $\vec{\mu}$ with respect to \mathfrak{p}_∞ (see [12, page 162]). Indeed, the normalization can be obtained by the change of variable $y_{ij} \mapsto y_{ij} + \alpha_{ij}$, $1 \leq i \leq r$, $1 \leq j \leq n$ where $\vec{y}_i = (y_{i1}, \dots, y_{in})$, $\vec{y}_i^p \dot{-} \vec{y}_i = \vec{\delta}_i$ and $\alpha_{ij} \in k$, that corresponds to the substitution $\delta_{ij} \mapsto \delta_{ij} + \alpha_{ij}^p - \alpha_{ij}$ and therefore the components obtained have no poles other than \mathfrak{p}_i . \square

Now we study the behavior of \mathfrak{p}_∞ in K/k .

Proposition 5.6. *Let K/k be given as in Theorem 5.5. Let $\mu_1 = \cdots = \mu_s = 0$, $\mu_{s+1} \in \mathbb{F}_q^*$, $\mu_{s+1} \notin \wp(\mathbb{F}_q)$ and finally, let $t+1$ be the first index with $f_{t+1} \notin \mathbb{F}_q$ (and therefore $p \nmid \deg f_{t+1}$). Then the ramification index of \mathfrak{p}_∞ is p^{n-t} , the inertia degree of \mathfrak{p}_∞ is p^{t-s} and the decomposition number of \mathfrak{p}_∞ is p^s . More precisely, if $\text{Gal}(K/k) = \langle \sigma \rangle \cong C_{p^n}$, then the inertia group of \mathfrak{p}_∞ is $\mathfrak{I} = \langle \sigma^{p^t} \rangle$ and the decomposition group of \mathfrak{p}_∞ is $\mathfrak{D} = \langle \sigma^{p^s} \rangle$.*

Proof. Since the extension K/k is a Galois extension of degree a power of a prime, the inertia field is the first layer such that \mathfrak{p}_∞ ramifies. The index of this first layer is $t+1$ (see [12]). On the other hand, by the same reason, the decomposition field is the first layer where \mathfrak{p}_∞ is inert and this is given by $s+1$ (Proposition 5.3). \square

Now $\vec{y}_i^p \dot{-} \vec{y}_i = \vec{\delta}_i$, $1 \leq i \leq r$ and $\vec{z}^p \dot{-} \vec{z} = \vec{\mu}$. Note that $k(\vec{y}, \vec{y}_i)$ and $k(\vec{y}, \vec{z})$ are unramified extensions of $k(\vec{y})$.

We have $k(\vec{y} \dot{-} \vec{z}) \subseteq k(\Lambda_N)$ for some $N \in R_T$ since by Proposition 5.6, \mathfrak{p}_∞ is fully decomposed in $k(\vec{y} \dot{-} \vec{z})$. Therefore $E = k(\vec{y} \dot{-} \vec{z})$ is contained in a cyclotomic function field.

If χ is the character associated to E , then $\chi = \chi_{P_1} \cdots \chi_{P_r}$, where each χ_{P_i} is of order p^{n_i} with $n_i \leq n$. Clearly, the field associated to χ_{P_i} is $k(\vec{y}_i)$. It follows that $E_g = k(\vec{y}_1, \dots, \vec{y}_r)$ since \mathfrak{p}_∞ is fully decomposed.

Note that $Kk(\vec{z})/K$ is unramified and $S_\infty(K)$ decomposes fully. It follows from Theorems 4.1 and 4.4 that $K_g = E_g k(\vec{z})$.

Therefore we have proved

Theorem 5.7. *If K/k is given as in Theorem 5.5, then $K_g = k(\vec{y}_1, \dots, \vec{y}_r, \vec{z})$ where $\vec{y}_i^p \dot{-} \vec{y}_i = \vec{\delta}_i$, $1 \leq i \leq r$ and $\vec{z}^p \dot{-} \vec{z} = \vec{\mu}$.* \square

Example 5.8. Let $k = \mathbb{F}_3(T)$ and $K = k(\vec{y})$ where $\vec{y}^3 \dot{-} \vec{y} = \vec{\beta} = (\frac{1}{T} + 1, \frac{1}{T+1} + T)$. Then the decomposition prescribed in Theorem 5.5 is:

$$\vec{\beta} = \left(\frac{1}{T}, \frac{T+1}{T^2} \right) \dot{+} \left(0, \frac{1}{T+1} \right) \dot{+} (1, T).$$

Thus, if $\vec{y}_1^3 \dot{-} \vec{y}_1 = \vec{\delta}_1 = (\frac{1}{T}, \frac{T+1}{T^2})$, $\vec{y}_2^3 \dot{-} \vec{y}_2 = \vec{\delta}_2 = (0, \frac{1}{T+1})$ and $\vec{z}^3 \dot{-} \vec{z} = \vec{\mu} = (1, T)$, then $K_g = k(\vec{y}_1, \vec{y}_2, \vec{z})$.

REFERENCES

- [1] Bae, Sunghan; Koo, Ja Kyung, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60**, no. 3, 301–310, (1996).
- [2] Clement, Rosario, *The genus field of an algebraic function field*, J. Number Theory **40**, no. 3, 359–375, (1992).
- [3] Fröhlich, Albrecht, *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics, **24**, American Mathematical Society, Providence, RI, 1983.
- [4] Gauss, Carl Friedrich, *Disquisitiones arithmeticae*, 1801.
- [5] Hasse, Helmut, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3**, 45–51, (1951).
- [6] Hu, Su; Li, Yan, *The genus fields of Artin–Schreier extensions*, Finite Fields Appl. **16**, no. 4, 255–264, (2010).
- [7] Ishida, Makoto, *The genus fields of algebraic number fields*, Lecture Notes in Mathematics, Vol. **555**, Springer-Verlag, Berlin-New York, 1976.
- [8] Leopoldt, Heinrich W., *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9**, 351–362, (1953).

- [9] Peng, Guohua, *The genus fields of Kummer function fields*, J. Number Theory **98**, no. 2, 221–227, (2003).
- [10] Rosen, Michael, *The Hilbert class field in function fields*, Exposition. Math. **5**, no. 4, 365–378, (1987).
- [11] Rosen, Michael, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York, 2002.
- [12] Schmid, Hermann Ludwig, *Zur Arithmetik der zyklischen p -Körper*, J. Reine Angew. Math. **176**, 161–167 (1936).
- [13] Villa Salvador, Gabriel Daniel, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.
- [14] Zhang, Xianke, *A simple construction of genus fields of abelian number fields*, Proc. Amer. Math. Soc. **94**, no. 3, 393–395, (1985).

DEPARTAMENTO DE MATEMÁTICAS, ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS DEL I.P.N.
E-mail address: `rosalia@esfm.ipn.mx`

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.
E-mail address: `mrzedowski@ctrl.cinvestav.mx`

DEPARTAMENTO DE CONTROL AUTOMÁTICO, CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS DEL I.P.N.
E-mail address: `gvilla@ctrl.cinvestav.mx`